



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
[www.uspto.gov](http://www.uspto.gov)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/613,522	07/02/2003	Liqun Chen	B-5153 621074-2	4783
7590	03/23/2007		EXAMINER	
HEWLETT-PACKARD COMPANY Intellectual Property Administration P.O. Box 272400 Fort Collins, CO 80527-2400			ABEDIN, SHANTO	
			ART UNIT	PAPER NUMBER
			2136	
SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE		
3 MONTHS	03/23/2007	PAPER		

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

<b>Office Action Summary</b>	<b>Application No.</b>	<b>Applicant(s)</b>	
	10/613,522	CHEN ET AL	
	<b>Examiner</b>	<b>Art Unit</b>	
	Shanto M Z Abedin	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

#### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 03 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

- 1) Responsive to communication(s) filed on 24 November 2006.
- 2a) This action is **FINAL**.                    2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

- 4) Claim(s) 1-17, 19-25, 27 and 28 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) Claim(s) \_\_\_\_\_ is/are allowed.
- 6) Claim(s) 1-17, 19-25, 27 and 28 is/are rejected.
- 7) Claim(s) \_\_\_\_\_ is/are objected to.
- 8) Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on \_\_\_\_\_ is/are: a) accepted or b) objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) All    b) Some \* c) None of:
  1. Certified copies of the priority documents have been received.
  2. Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)            | 4) <input type="checkbox"/> Interview Summary (PTO-413)           |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)   | Paper No(s)/Mail Date. _____.                                     |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date <u>07/02/2003, 11/13/2006</u> .                                  | 6) <input type="checkbox"/> Other: _____.                         |

## DETAILED ACTION

1. This office action is in response to the communication filed on 11/24/2006.
2. The examiner acknowledges and accepts the drawings filed on 07/02/2003.
3. The examiner acknowledges that this application claims priority to an earlier application filed on July 5, 2002.
4. The applicant's representative elected group 1 (claims 1-17, 19-25, 27-28) in response to an earlier restriction/ election requirement mailed on 10/31/2006.
5. Claims 1-17, 19-25, 27-28 are now pending in the application.
6. Claims 1-17, 19-25 and 27-28 have been rejected.

### ***Claim Rejections - 35 USC § 101***

35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

7. Claims 1-5, 12-17, 25, and 27-28 are rejected under 35 U.S.C. §101 because claimed invention as a whole either fails to accomplish a practical/ useful application, or directed to a program per se product.

***Regarding claims 1-5, 12-17 and 25,*** the features and the elements of the claims merely represent an abstract/ mathematical idea, or manipulation of abstract/ mathematical idea – they lack producing required useful/ practical results. Therefore, the claims are non statutory under 35 U.S.C. 101 as not being useful (MPEP § 2106).

***Regarding claims 27-28,*** they are rejected as being non statutory since they merely disclose producing non function data, or a program per se product (MPEP § 2106.01 [R-5]).

***Claim Rejections - 35 USC § 102***

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

8. Claims 1-17, 19-25, 27-28 are rejected under 35 USC 102 (e) as being anticipated by Gentry et al (US 2003/ 0182554 A1).

***Regarding claims 1 and 27, Gentry et al*** discloses a method/ computer program product of enabling a third party to verify an association between a first party associated with a first element, of a first algebraic group, and a second party associated with a second element, of a second algebraic group, formed from an identifier string of the second party, wherein:

there exists a computable bilinear map for the first and second elements; the first party has a first secret and computes a first product from the first secret and the first element (Par [0010], [0011], [0019], [0024]; first secret elements)

the second party has both a second secret, and a shared secret provided by the first party as the product of the first secret and the second element (Par [0011], [0019], [0024]; second secret elements);

the second party computes first, second and third verification parameters as the product of the second secret with said shared secret, the second element and the first element respectively

Art Unit: 2136

([0010], [0011], [0024]; Claims 1-3; determining first, second intermediate shared secret, and interactive shared secret).

***Regarding claims 8, 22 and 28,*** Gentry et al discloses a method/ apparatus/ computer program product of verifying an association between a first party associated with a first element, of a first algebraic group, and a second party associated with a second element, of a second algebraic group; the first and second elements being such that there exists a bilinear mapping p for these elements; the method comprising carrying out the following operations:

receiving both data indicative of said first element, and a first product formed by the first party from a first secret and the first element (Par [0011], [0019], [0024]; first and second secret elements);

receiving in respect of the second party both an identifier string, and first, second and third verification parameters (Par [0022], [0024]; Claim 1; first and second secrets and system parameter);

computing the second element from the identifier string of the second party; carrying out a first check:  $p$  (third verification parameter, computed second element)= $p$  (first element, second verification parameter) (Par [0028], [0033], Claim 11, 18, 19;determining)

carrying out a second check:  $p$  (first element, first verification parameter)= $p$  (first product, second verification parameter) (Par [0028], [0033], Claim 11, 18, 19;determining)

the association between the first and second parties being treated as verified if both checks are passed (Par [0028], [0033]; Claim 19; authentication).

***Regarding claim 12,*** Gentry et al discloses method of enabling verification of an association between parties, the method comprising:

generating a first private key and public key for a first party (par [0003], [0022]; generating private, public keys);

generating a second private and public key for a second party wherein the second private key is derived from the first private key and second public key (par [0003], [0022]); and

generating a third private key for the second party that is used in association with the first public key, the second private key and the second public key to form a first cryptographic parameter, a second cryptographic parameter and a third public key respectively (Par [0022], Claim 6,12; private, public keys; first and second secrets).

*Regarding claim 19*, it recites the limitations of claim 1, therefore, it is rejected applying as above rejecting claim 1, furthermore, Gentry et al discloses apparatus arranged to enable a third party to verify an association between the apparatus and a first party that has a first secret and is associated with a first element of a first algebraic group, the apparatus being associated with a second element, of a second algebraic group, and the first and second elements being such that there exists a bilinear mapping p for these elements; the apparatus comprising:

a memory for holding a second secret and an identifier string associated with the apparatus (Par [0010], Claim 18, 19; memory),

means for forming said second element from said identifier string (Par [0041]; Claim 18, 19; processor),

means for receiving from the first party a shared secret based on said first secret and said first element, and for storing this shared secret in the memory (Claim 1,6,18; entity; communicating),

means for computing first, second and third verification parameters as the product of the second secret with said shared secret, said second element and said first element respectively (Par [0041]; Claim 18, 19; processor), and

means for making available said identifier string and said verification parameters to the third party (Par [0041]; Claim 18, 19; processor).

*Regarding claim 25, Gentry et al* discloses a hierarchy of trusted authorities wherein:

each trusted authority is associated with a point on an elliptic curve, this point being derived, at least for each non-root trusted authority, from an identifier string of the trusted authority (Par [0003], [0004]; deriving keys from master secret; trusted party);

at least the non-leaf trusted authorities each has a standard elliptic-curve public/private key pair wherein the private key is formed by a secret of the trusted authority concerned and the public key comprises the product of this secret with the point associated with that trusted authority (Par [0003], [0004]; claim 6-7; elliptic curve; shared secret);

at least the non-root trusted authorities each has an identifier-based elliptic-curve public/private key pair wherein the public key comprises the identifier string of the trusted authority concerned and the private key is a shared secret provided by a said trusted authority at a next level up in the hierarchy, the shared secret being the product of the secret of the next-level-up trusted authority and the point associated with the trusted authority to which the shared secret is provided (Par [0021], [0022], [0040]; Claim 18, 19; root level/ master secret; authentication; trusted party); and

at least the non-root trusted authorities each has two further public parameters formed by the product of the secret of the trusted authority respectively with the shared secret provided to it by the next-level-up trusted authority and with the point associated with the latter (Par [0021], [0040]; Claims 1-3, 18, 19; determining first, second intermediate shared secret, and interactive shared secret).

***Regarding claim 2, Gentry et al*** discloses method a wherein the second party generates a further shared secret from the second secret and an identifier string of a fourth party, the second party passing this further shared secret to the fourth party for use by the latter as the private key of a public/private key pair the public key of which is formed by the identifier string of the fourth party (Par [0040]; system including multiple entities).

***Regarding claim 3, Gentry et al*** discloses a method wherein the first and second parties are respectively parent and child trusted authorities in a hierarchy of trusted authorities (Par [0003], [0004]; trusted party).

***Regarding claim 4, Gentry et al*** discloses a method wherein the first and second algebraic groups are the same (Par [0019]; algebraic groups).

***Regarding claim 5, Gentry et al*** discloses a method wherein the first and second elements are points on the same elliptic curve (Par [0019]; elliptic curves).

***Regarding claim 6,*** Gentry et al discloses method of verifying an association between the first and second parties of claim 1 by using a function p providing said bilinear map; the method comprising carrying out the following operations using the non-secret data elements of claim 1:

computing the second element from the identifier string of the second party (Par [0028, [0033], Claim 18; second shared secret])

carrying out a first check: p (third verification parameter, computed second element)=p (first element, second verification parameter) (Par [0028, [0033], Claim 11, 18;determining)

carries out a second check: p (first element, first verification parameter)=p (first product, second verification parameter) (Par [0028, [0033], Claim 11, 18;determining)

the association between the first and second parties being treated as verified if both checks are passed (Par [0028, [0033], authentication).

***Regarding claim 7,*** Gentry et al discloses the method wherein said bilinear mapping function is based on a Tate or Weil pairing (Par [0021]; Tate or Weil pairing).

***Regarding claim 9-11,*** they recite the limitations of claims 4-5 and 8, therefore, they are rejected applying as above rejecting claims 4-5 and 8.

***Regarding claim 13,*** Gentry et al discloses the method wherein a third party uses the first, second and third cryptographic parameters together with the first and second public keys to check, by using bilinear mapping, whether there is an association between the first and second parties (Par [0022], Claim 6,12).

***Regarding claim 14, Gentry et al*** discloses the method wherein the bilinear mapping is based on either a Tate or Weil pairing (Par [0021]).

***Regarding claim 15, Gentry et al*** discloses the method wherein the third private key is combined with a third party's public key to form an associated private key such that an association can be established between the third public key of the second party and the first public key of the first party (Par [0022], Claim 6,12).

***Regarding claim 16, Gentry et al*** discloses the method wherein the third private key is a random number (Par [0022], Claim 6,12; random integer/ number).

***Regarding claim 17, Gentry et al*** discloses the method wherein the first party is a first trusted party and the second party is a second trusted party (Par [0003], [0004]; trusted party).

***Regarding claim 20-21 and 23-24,*** they recite the limitations of claims 4-5 and 19, therefore, they are rejected applying as above rejecting claims 4-5 and 19.

### ***Conclusion***

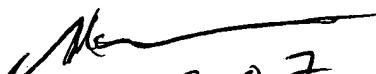
9. A shortened statutory period for response to this action is set to expire in 3 (Three) months and 0 (Zero) days from the mailing date of this letter. Failure to respond within the period for response will result in ABANDONMENT of the application (see 35 U.S.C 133, M.P.E.P 710.02(b)).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shanto M Z Abedin whose telephone number is 571-272-3551. The examiner can normally be reached on M-F from 9:00 AM to 5:30 PM. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Moazzami Nasser, can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Shanto M Z Abedin  
Examiner, AU 2136

NASSER MOAZZAMI  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100

  
3,19,07